SSA-183963: Certificate Validation Vulnerabilities in SICAM TOOLBOX II Before V07.11

Publication Date: 2025-07-08
Last Update: 2025-07-08
Current Version: V1.0
CVSS v3.1 Base Score: 8.1
CVSS v4.0 Base Score: 7.7

SUMMARY

During establishment of a https connection to the TLS server of a managed device, SICAM TOOLBOX II improperly validates that device's certificate. This could allow an attacker to execute an on-path network (MitM) attack.

Siemens has released a new version for SICAM TOOLBOX II and recommends to update to the latest version.

The chapter "Additional Information" provides additional guidance how to prevent on-path network attacks.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM TOOLBOX II: All versions < V07.11 affected by all CVEs	Update to V07.11 or later version https://support.industry.siemens.com/cs/ww/en/view/109822197/

WORKAROUNDS AND MITIGATIONS

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design. Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment. As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines can be found at: https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SICAM TOOLBOX II is an engineering solution for plants and systems of all sizes. It allows data collection, data modeling, configuration, and parameterization. It is used for engineering of process information for the automation and central control-room systems.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-31853

During establishment of a https connection to the TLS server of a managed device, the affected application doesn't check the extended key usage attribute of that device's certificate. This could allow an attacker to execute an on-path network (MitM) attack.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	7.7
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2024-31854

During establishment of a https connection to the TLS server of a managed device, the affected application doesn't check device's certificate common name against an expected value. This could allow an attacker to execute an on-path network (MitM) attack.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	7.7
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-295: Improper Certificate Validation

ADDITIONAL INFORMATION

Additional guidance for SICAM TOOLBOX II users to prevent from on-path attacks:

The fix for CVE-2024-31854 only works with the devices CP-8000/8021/8022, CP-8050/31 and SICAM AK3 and if the latest firmware is installed on them (ability to trust the current certificate of the device and maintain the corresponding "trust" in SICAM TOOLBOX II). For details see the V07.11 release notes and the SICAM TOOLBOX II Help and Administrator manual.

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2025-07-08): Publication Date

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.